

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Masayuki NUMAO et al.

Serial No: 10/600,547

Filed: June 20, 2003

For: INFORMATION  
DISTRIBUTION AND PROCESSING

Examiner: MORSE,  
Gregory A.

Art Unit: 2134

**APPEAL BRIEF**

Board of Patent Appeals and Interferences  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

The applicant submits this brief pursuant to 37  
C.F.R. §41.37(a)(1) in furtherance of the Notice of Appeal  
filed January 26, 2009.

Please apply the appeal brief fee paid January 4,  
2008 to cover the required fee for filing this Notice of  
Appeal, in accordance with MPEP 1204.01. No additional  
fee is believed due with this Appeal Brief, however,  
should such a fee be required please charge Deposit  
Account 50-0510.

### **Real Party in Interest**

The real party in interest is International Business Machines Corporation.

### **Related Appeals and Interferences**

The Appellants' legal representative does not know of any other appeal, interference or judicial proceeding which will affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

### **Status of Claims**

Claims 1-10, 20 and 21 are pending in the present application, with claims 1, 4, 6, 9, 20 and 21 being independent claims. Claims 11-19 and 22-25 are cancelled. The rejection of claims 1-10, 20 and 21 is appealed.

### **Status of Amendments**

No amendments to the claims were made after the Final Office Action dated September 24, 2008 ("FOA").

### **Summary of the Claimed Subject Matter**

Independent claim 1 recites an information distribution system. App., [0032], Fig. 1. The information distribution system includes a key management server for managing secret keys and public keys corresponding to given attribute values. App., [0061], Fig. 1, item 10. A user terminal accesses the key management server to obtain attribute secret keys generated based on the secret keys. App., [0062], Fig. 1, item 30. Furthermore, the attribute secret keys

correspond to attributes identifying the user terminal.  
App., [0050].

Claim 2 is dependent on claim 1 and recites that the provider terminal distributes the encrypted content without specifying an address of the user terminal that is to receive the encrypted content. App., [0115].

Independent claim 4 recites a server that includes a key storage for storing secret keys and public keys corresponding to predetermined attribute values. App., [0050] and Fig. 2, item 12. The server also includes an attribute secret key generator for obtaining a set of given attribute values and generating attribute secret keys corresponding to the set of attribute values based on secret keys corresponding to the attribute values among the secret keys stored in the key storage. App., [0050] and Fig. 2, item 11. A sending/receiving unit receives the set of attribute values from a given user terminal and sends the attribute secret keys generated by the attribute secret key generator to the user terminal. App., [0033]. Furthermore, the attribute values identify the user terminal. App., [0045].

Independent claim 6 recites an information processing apparatus that includes a criteria key generator for obtaining public keys corresponding to attribute values indicating attributes identifying a recipient to which a content is to be sent and using the public keys to generate criteria keys that can be decrypted by secret keys corresponding to the public keys. App., [0034], [0087] and Fig. 2, item 22. The apparatus also includes an encrypted content generator for encrypting the content

based on the criteria keys. App., [0052] and Fig. 2, item 21. Furthermore, a sending unit is used to send the encrypted content without specifying any recipient of the content via a network. App., [0034].

Independent claim 9 recites an information processing apparatus receiving a content distributed over a network. App., Fig. 1. The apparatus includes a sending/receiving unit for accessing a key management server managing secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for identifying the information processing apparatus. App., [0036]. The attribute secret keys are generated based on the secret keys. App., [0036]. A decryptor is used to obtain an encrypted content and decrypt the content based on the attribute secret keys. App., [0054] and Fig. 2, item 32.

Independent claim 20 recites an information distribution system including a service provider managing secret keys and public keys for given attribute values. App., [0039], Fig. 8, item 800. The system also includes a plurality of user terminals for accessing the service provider to obtain attribute secret keys corresponding to attributes identifying the user terminals. App., [0039], [0062], Fig. 1, item 30. The attribute secret keys are generated based on the secret keys. App., [0036]. Furthermore, a given one of the user terminals generates an encrypted content and sends the encrypted content to one or more of the other user terminals. App., [0041], Fig. 8, item 810. The encrypted content is decryptable by the other user terminals having the attribute secret keys

corresponding to given attributes by means of the public keys. App., [0040].

Independent claim 21 recites an information distribution system including a key management server for managing secret keys and public keys for given attribute values. App., [0061], Fig. 1, item 10. The system also includes a plurality of user terminals for accessing the key management to obtain attribute secret keys corresponding to attributes identifying the user terminals. App., [0039], [0062], Fig. 1, item 30. The attribute secret keys are generated based on the secret keys. App., [0036]. Furthermore, a given one of the user terminals generates a group key and sends the group key to one or more of the other user terminals and provides a content. App., [0040], Fig. 10, item 1010. The encrypted group key is decryptable by the other user terminals having the attribute secret keys corresponding to given attributes by means of the public keys. App., [0040].

#### **Grounds for Rejection to be Reviewed on Appeal**

I. Claims 1, 3, 4, 6-10, 20 and 21 are rejected under 35 U.S.C. § 103 as unpatentable over U.S. Patent No. 6,215,877 issued to Matsumoto ("Matsumoto") in view of U.S. Patent Publication No. 2001/0004736 ("Hirano").

II. Claim 2 is rejected under 35 U.S.C. § 103 as obvious over Matsumoto in view of Hirano and U.S. Patent No. 5,933,605 issued to Kawano et al. ("Kawano").

III. Claim 5 is rejected under 35 U.S.C. § 103 as obvious over Matsumoto in view of Hirano and "Applicant Admittance Prior Art."

### **Argument**

#### **I. CLAIMS 1, 3, 4, 6-10, 20 AND 21 ARE NOT OBVIOUS UNDER 35 U.S.C. § 103 OVER MATSUMOTO IN VIEW OF HIRANO**

##### Claim 1

The present application relates to an information distribution system that allows message producers to contact message consumers meeting certain criteria without revealing addresses of the message consumers to third parties, including the message sender. App., [0031]. This is performed by encrypting the message with one or more keys corresponding to attributes of the message consumer. App., [0032]. For example, message contents can be encrypted using secret keys based on the attributes "gender (male) & age (30's) & occupation (office worker) & (hobby (travel) | hobby (PC operation))." App., [0048]. The message can only be decrypted by a message consumer having public keys corresponding to the same attributes. App., [0039].

Claim 1 recites, in part, "a key management server for managing secret keys and public keys corresponding to given attribute values." Furthermore, the specification states, "The term attribute as used herein refers to information representing the individuality of the user of a user terminal 30 or the user terminal itself." App., [0046]. Thus, Appellants submit the term attribute must

be interpreted from the specification to mean information representing the individuality of a user of a user terminal or the user terminal itself.

In the Final Office Action, Matsumoto (the primary reference) is cited as disclosing a key management server for managing secret keys and public keys corresponding to given attribute values. FOA, pp. 3-4. However, the Appellants submit that the Examiner fails to properly determine the meaning of terms used in the claim.

Matsumoto relates to a chat system including a key management server for supplying a key to the encryption of the communication. Matsumoto, col. 1, ll. 5-11. The communication is encrypted based on the communication channel used. Matsumoto, col. 6, ll. 28-31. Thus, Matsumoto is distinguished from claim 1 because the encryption key used does not correspond to information representing the individuality of the user of a user terminal or the user terminal itself, but rather the communication channel used.

Claim 1 further recites, part in, "a user terminal for accessing said key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes identifying said user terminal." The Examiner correctly notes that Matsumoto fails to disclose a user terminal as claimed. However, Hirano is cited by the Examiner to overcome the deficiencies of Matsumoto. The Appellants respectfully disagree with the Examiner.

Hirano discloses a system for encrypting digital

content. Hirano, para. [0068]. According to Hirano, "[T]he content user decrypts the authorization information 63 to pick out a content key 64 and image-compositing information 65. . . . On this account, the content user 3 creates a decryption key 66 corresponding to the secret key 47 based on such user information 14 as: user identification information . . . ." Hirano, para. [0098] (emphasis added). Hirano discloses the content user generates a decryption key corresponding to a secret key based on user identification information. Moreover, the content user never obtains the secret key. Only the authorization information encrypted by the secret key is obtained by the content user.

By contrast, claim 1 recites a user terminal that accesses the key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes identifying said user terminal. Hirano fails to disclose a system where a user terminal accesses a key management server to obtain attribute secret keys corresponding to attributes identifying said user terminal.

Finally, the only rational put forth in the Final Office Action for modifying the teachings of Matsumoto with that of Hirano is that "it offers the advantage of protecting computerized data from unauthorized access." FOA, pp. 4. However, as discussed above, Matsumoto already discloses encrypting communication based on the communication channel used. Thus, the argument in the Final Office Action for combining Matsumoto and Hirano lacks merit. It is apparent that the only rational for



combining Matsumoto and Hirano in the manner advanced by the Examiner stems from hindsight knowledge impermissibly derived from the Appellants' disclosure.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 1. The Appellants submit that the rejection of claim 1 is in error and respectfully request that the rejection of claim 1 be reversed by the Honorable Board.

#### Claim 3

If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

Claim 3 is dependent on and further limits claim 1. Since the rejection of claim 1 is believed in error, the rejection of claim 3 is also believed in error for at least the same reasons as claim 1.

#### Claims 4, 6, 9, 20 and 21

Claims 4, 6, 9, 20 and 21 were rejected for similar reasoning as claim 1. Thus, claims 4, 6, 9, 20 and 21 are believed allowable for at least the same reasons as claim 1.

#### Claims 7 and 8

Claims 7 and 8 are dependent on and further limit claim 6. Since the rejection of claim 6 is believed in error, the rejection of claims 7 and 8 is also believed in error for at least the same reasons as claim 6.

#### Claim 10

Claim 10 is dependent on and further limits claim 9. Since the rejection of claim 9 is believed in error, the rejection of claim 10 is also believed in error for at least the same reasons as claim 9.

**II. CLAIM 2 IS NOT OBVIOUS UNDER 35 U.S.C. § 103 OVER MATSUMOTO IN VIEW OF HIRANO AND KAWANO**

Claim 2 recites, "The information distribution system according to claim 1, wherein said provider terminal distributes said encrypted content without specifying an address of said user terminal that is to receive said encrypted content."

In rejecting claim 2, the Examiner acknowledges Matsumoto fails to disclose the subject matter of claim 2, but alleges such teaching can be found in Kawano (U.S. Patent No. 5,933,605). FOA, pg. 8. Specifically, the Examiner points to column 11, lines 40-57 of Kawano.

The Kawano passage cited by the Examiner states,

In the communication system using the contents code, the transmitting computer attaches to the transmission data the contents code corresponding to the contents of transmission data and then transmits the resultant data without recognizing the address of the party. A receiving computer sets data to be received on the basis of the contents code of the transmission data. Thus, the receiving computer can execute its operation without recognizing the position of itself and number of the computers as an [sic] transmission originator of the transmission data while taking only the data contents into consideration. Since each computer receives data while not specifying the data transmission originator, it is only required to broadcast the transmission data within the system and for the receiving computer to receive the data alone attached

to the coincidence contents code. As a result, the data receiving operation can be carried out independently of the expansion of the system such as addition or deletion of a transmitting computer. Kawano, col. 11, ln. 40-57.

According to Kawano, a transmitting computer attaches to the transmission data the contents code corresponding to the contents of transmission data and then transmits the resultant data without recognizing the address of the party. The citation makes no mention of a provider terminal distributing encrypted content without specifying an address of a user terminal that is to receive the encrypted content.

"Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336, quoted with approval in KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007).

The Examiner provides no explanation or reasoning for the rejection beyond merely citing column 11, lines 40-57 of Kawano why the limitations of claim 2 are disclosed in Kawano. Thus, the rejection of amounts to a conclusory statement unsupported by articulated reasoning or rational underpinning. See 37 C.F.R. 1.104(c)(2).

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of unpatentability for claim 2. The Appellants submit that the rejection of claim 2 is in

error and respectfully request that the rejection of claim 2 be reversed by the Honorable Board.

**III. CLAIM 5 IS NOT OBVIOUS UNDER 35 U.S.C. § 103**  
**MATSUMOTO IN VIEW OF HIRANO AND "APPLICANT ADMITTANCE**  
**PRIOR ART"**

Claim 5 is dependent on and further limits claim 4. Since the rejection of claim 4 is believed in error, the rejection of claim 5 is also believed in error for at least the same reasons as claim 4.

**Conclusion**

In view of the foregoing, Appellant submits that the rejections of claims 1-10, 20 and 21 are improper and respectfully requests that the rejections of claims 1-10, 20 and 21 be reversed by the Honorable Board.

Dated: March 26, 2008

Respectfully submitted,

/ido tuchman/  
Ido Tuchman, Reg. No. 45,924  
Law Office of Ido Tuchman  
82-70 Beverly Road  
Kew Gardens, NY 11415  
Telephone (718) 544-1110  
Facsimile (718) 374-6092

## **Claims Appendix**

Claim 1. (previously presented) An information distribution system comprising:

- a key management server for managing secret keys and public keys corresponding to given attribute values;

- a user terminal for accessing said key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes identifying said user terminal; and

- a provider terminal for generating an encrypted content that can be decrypted by said user terminal having said attribute secret keys corresponding to given attributes by means of said public keys;

wherein said provider terminal distributes said encrypted content and said user terminal decrypts said encrypted content decryptable by means of said attribute secret keys of its own.

Claim 2. (previously presented) The information distribution system according to claim 1, wherein said provider terminal distributes said encrypted content without specifying an address of said user terminal that is to receive said encrypted content.

Claim 3. (original) The information distribution system according to claim 1, wherein said user terminal sends a set of attribute values indicating attributes of its own to said key management server; and

said key management server generates said attribute secret keys unique to said user terminal based on, among said secret keys managed by said key management server, secret keys corresponding to the attribute values sent from said user terminal and sends said attribute secret keys to said user terminal.

Claim 4. (previously presented) A server comprising:  
a key storage for storing secret keys and public keys corresponding to predetermined attribute values;

an attribute secret key generator for obtaining a set of given attribute values and generating attribute secret keys corresponding to said set of attribute values based on secret keys corresponding to said attribute values among said secret keys stored in said key storage; and

a sending/receiving unit for receiving said set of attribute values from a given user terminal and sending said attribute secret keys generated by said attribute secret key generator to said user terminal; and

wherein said attribute values identifying said user terminal.

Claim 5. (previously presented) The server according to claim 4, wherein said attribute secret key generator generates said attribute secret keys by using a protocol implementing oblivious transfer protocol.

Claim 6. (previously presented) An information processing apparatus comprising:

a criteria key generator for obtaining public keys corresponding to attribute values indicating attributes identifying a recipient to which a content is to be sent and using said public keys to generate criteria keys that can be decrypted by secret keys corresponding to said public keys;

an encrypted content generator for encrypting said content based on said criteria keys; and

a sending unit for sending said encrypted content without specifying any recipient of said content via a network.

Claim 7. (original) The information processing apparatus according to claim 6, wherein said criteria key generator combines, based on predetermined rules, criteria keys corresponding to the individual attribute values encrypted by using public keys corresponding to said individual attribute values to generate a criteria key for restricting recipients of said content.

Claim 8. (original) The information processing apparatus according to claim 6, wherein said criteria key generator generates a session key for encrypting said content and a criteria key for decrypting said session key; and

said encrypted content generator uses said session key to encrypt said content.

Claim 9. (previously presented) An information processing apparatus receiving a content distributed over a network, comprising:

a sending/receiving unit for accessing a key management server managing secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for identifying said information processing apparatus, said attribute secret keys being generated based on said secret keys; and

a decryptor for obtaining an encrypted content and decrypting said content based on said attribute secret keys.

Claim 10. (currently amended) The information processing apparatus according to claim 9, wherein said sending/receiving unit sends a set of attribute values established for said information processing apparatus to said key management server and receives said attribute secret keys generated based on said set of attribute values from said key management server.

Claims 11-19. (cancelled)

Claim 20. (previously presented) An information distribution system comprising:

a service provider managing secret keys and public keys for given attribute values; and

a plurality of user terminals for accessing said



service provider to obtain attribute secret keys corresponding to attributes identifying the user terminals, said attribute secret keys being generated based on said secret keys;

wherein, a given one of said user terminals generates an encrypted content and sends said encrypted content to one or more of the other user terminals, said encrypted content being decryptable by said one or more of the other user terminals having said attribute secret keys corresponding to given attributes by means of said public keys; and

said one or more of the other user terminals decrypt said encrypted content decryptable by means of said attribute secret keys of their own.

Claim 21. (previously presented) An information distribution system comprising:

a key management server for managing secret keys and public keys for given attribute values; and

a plurality of user terminals for accessing said key management server to obtain attribute secret keys corresponding to attributes identifying the user terminals, said attribute secret keys being generated based on said secret keys, wherein a given one of said user terminals generates a group key and sends said group key to ones of the other user terminals and provides a content, said encrypted group key being decryptable by said ones of the other user terminals having said attribute secret keys corresponding to given attributes by

means of said public keys, said content being only accessible by using said group key.

Claims 22-25. (cancelled)

## **Evidence Appendix**

None.

## **Related Proceedings Appendix**

None.